

Shared: Data Retention

Setup Guide for Concur Standard Edition

Last Revised: January 30, 2024

Applies to these SAP Concur solutions:

- Expense
 - Professional/Premium edition
 - Standard edition

- Travel
 - Professional/Premium edition
 - Standard edition

- Invoice
 - Professional/Premium edition
 - Standard edition

- Request
 - Professional/Premium edition
 - Standard edition

Table of Contents

- Section 1: Permissions 1**
- Section 2: Overview 1**
 - Required Client-Driven Components 2
 - Profile Data Purge 2
 - Data Retention Policy Purge..... 2
 - Feature Benefits..... 4
 - Terminology 5
 - Data Retention Roles 6
 - What the Admin Sees 6
- Section 3: How It Works 8**
 - Please Note the Following..... 8
 - Creating a Company Data Retention Plan 8
 - Factoring Your Time Range to Retain or Remove Credit Card Data..... 8
 - For Clients Who Use the Employee Import Feature 8
 - Overview Steps..... 9
 - FAQs 9
 - Time Measurement..... 10
 - Determining the Age of the Data 10
 - Retention Periods 13
 - 72-Hour Activation Waiting Period 14
 - The 23-Month Filter 15
 - Unusual Scenarios..... 15
 - Request 15
- Section 4: Administrator Experience 16**
- Section 5: Activation 17**
- Section 6: Configuration 18**
 - Overview..... 18
 - Users who Change Policy Groups..... 18
 - Access the Data Retention Pages..... 19
 - Configure the Data Retention Periods..... 19
 - Edit the Data Retention Periods..... 25
- Section 7: Monitoring 25**
 - Configuration Changes..... 25
 - Email Confirmation of Pending Changes 26
 - View Pending Changes 26
 - Discard Pending Changes 27

Removed Data	28
Resources	29
Requesting a Report on Who is Viewing and Changing Personal Data	29
Change Logging Access	29
View Logging Access.....	29

Revision History

Date	Notes/Comments/Changes
January 30, 2024	Updated screen shots to reflect UI text change to "Profile Data".
January 9, 2024	Updated the <i>How it Works</i> section
September 13, 2023	Updated entire <i>Overview</i> section
September 7, 2023	Removed references to Purge User action.
May 11, 2023	Updated description of Purge User button on page 4.
May 25, 2022	The <i>Change Logging Access</i> section is renamed to <i>Requesting a Report on Who is Viewing and Changing Personal Data</i> and updated to explain how to request a report detailing who may have viewed a user's personal data.
May 20, 2022	In the <i>Configuration > Configure the Data Retention Periods</i> section, updated the note about best practices for configuring Concur Request retention period(s).
April 29, 2022	Added note about max limit of 1000 users on hold.
January 21, 2022	Updated the copyright year; no other changes; cover date not updated
November 29, 2021	Updated to add information about Change Logging access.
September 10, 2021	Updated to specify that user data can be purged from a Test environment.
April 15, 2021	Updated the copyright year; no other changes; cover date not updated
January 12, 2021	Added an FAQ question and section in the "Please Note the Following" section regarding how Employee Import can impact Data Retention for sensitive data. Also added three important notes regarding this topic.
December 8, 2020	Clarified the definition of the differences in the age of a Credit Card account.
April 27, 2020	Renamed the Authorization Request check box to Request on the guide's title page; cover date not updated
January 15, 2020	Updated the copyright; no other changes; cover date not updated
March 15, 2019	Added an IMPORTANT note to the <i>Activation</i> section. Added FAQs to the <i>How it Works</i> section. Other minor edits for clarity.
February 12, 2019	Updated the copyright; no other changes; cover date not updated
October 20, 2018	Updated graphics to reflect minor UI enhancements in the wizard. Added important notes about processing older transactions prior to enabling this feature to the <i>How it Works Overview Steps</i> section, <i>The 23-Month Filter</i> section, and the <i>Activation</i> section.
July 24, 2018	Clarified <i>The 23-Month Filter</i> section to indicate that the "View transactions" is "View (unassigned) transactions."
July 3, 2018	Added the following statement to the Overview section: "This feature is available for clients in our production environment but is not available for test or implementation entities."

Date	Notes/Comments/Changes
June 20, 2018	Corrected the math for example in the <i>Retention Periods</i> section on page 10.
June 6, 2018	Added detail to the <i>Data Retention Permissions/Roles</i> section regarding the need to pre-existing permissions/roles.
May 30, 2018	Added the <i>Activation</i> section.
May 12, 2018	Initial publication.

Data Retention

NOTE: Multiple SAP Concur product versions and UI themes are available, so this content might contain images or procedures that do not precisely match your implementation. For example, when SAP Fiori UI themes are implemented, home page navigation is consolidated under the SAP Concur Home menu.

Section 1: Permissions

A company administrator may or may not have the correct permissions to use this feature. The administrator may have limited permissions, for example, they can affect only certain groups and/or use only certain options (*view* but not *create* or *edit*).

If a company administrator needs to use this feature and does not have the proper permissions, they should contact the company's Concur administrator.

The administrator should be aware that some of the tasks described in this guide can be completed only by Concur. In this case, the client must initiate a service request with SAP Concur support.

Section 2: Overview

The Data Retention feature enables clients to control how long SAP Concur stores their data based on who, when, and where criteria.

By configuring this feature, clients can address requirements to comply with data privacy regulations by removing data. This feature removes data by anonymizing or deleting the data.

NOTE: Anonymization and deletion are employed for security and privacy purposes.

In the context of data protection, anonymization removes direct and indirect personal identifiers that can identify an individual. Anonymization is not reversible.

This feature is available for clients in both our production and test (Implementation) entities.

The Data Retention feature does not delete data directly. The various product areas execute the actual removal of the data for their product. For example, Concur Travel, Concur Expense, Concur Invoice, and Concur Request teams manage their own data, including anonymization and deletion.

For each client that has configured Data Retention Policies, the age of their data is calculated on a nightly basis. (Refer to the *Determining the Age of the Data* section in this document for a calculation table). The applicable product teams then execute anonymization or deletion of the eligible data. This process occurs for users' transactional data regardless of their status (active or inactive).

Required Client-Driven Components

The Data Retention feature has two required client-driven components:

- Profile Data Purge
- Data Retention Policy Purge

Profile Data Purge

The Profile Data Purge removes profile data in two intervals:

1. The first interval removes all profile data that has no bearing on the referential integrity of the user's transactional history. This includes (but is not limited to) data such as the user's email address, passport number, emergency contact information, and travel preferences for airlines, hotels, and rental car agencies.

The user's name and user ID are retained at this point to maintain referential integrity with corresponding transactional data that has not yet been removed or anonymized.

2. The second interval removes or anonymizes the remaining profile data after the longest Data Retention Policy period has elapsed. The user's name is deleted and their login ID and employee ID are anonymized with a Universally Unique Identifier (UUID).

NOTE: UUIDs are universally accepted as being globally unique due to the 36-character string that contains numbers, letters, and dashes.

Data Retention Policy Purge

The Data Retention Policy Purge removes non-profile related data described in the subsections below. The longest Data Retention Policy configuration will determine when the remaining profile data is removed and anonymized.

AUDIT

Audit Tasks related to identified Users are deleted. Deleted tasks include but are not limited to:

- All the data contained in the associated expense report.
- OCR text of any receipts that have been attached to the expense report.
- Results of auditing that has been performed on the expense report.

BANKING

All bank account details related to identified users, including secondary account data, is anonymized or deleted. This includes but is not limited to:

- Routing number, account number, name on account.

- Bank name, branch location, address, tax ID.
- Occupation, citizenship, and date of birth.

CASH ADVANCE

All Cash Advance details related to identified users that are contained in associated cash advance requests and issued cash advances (used or unused) are deleted.

CREDIT CARD

All Credit Card transactions related to identified users are deleted in accordance with the configured retention timeframe. Card transactions are deleted after expense entries are deleted. If the last transaction related to a card account is deleted, then the account(s) is also deleted. Additionally, unowned card data is deleted if it is older than the global retention timeframe.

EXPENSE REPORT

All Expense Report data related to identified users are deleted when their associated expense reports are deleted. The Expense Report details include but are not limited to:

- Report Header content, Report Entry content, Allocation content, and Cash Advance reference.

ITINERARY

All itinerary data related to identified users are deleted when their associated expense reports are deleted or if there is an unused itinerary. Itineraries contain but are not limited to:

- Company ID, User ID, Dates/times, departure and arrival location, addresses, itinerary ID, description, lodging details, and cross border details.

MILEAGE

All Journey Logs, Routes, and registered vehicles related to identified users are deleted.

Journey Logs include but are not limited to:

- Company ID, User ID, Report ID, Entry ID, Vehicle URL, route URL, odometer (start, end), calculation values, and journey date.

Routes include but are not limited to:

- User ID, Route ID, avoid highways, avoid tolls, unit, polyline (actual route data), and segments.

Vehicle data includes but is not limited to:

- Company ID, User ID, vehicle ID, description, deleted, preferred, properties (ownership type, engine size, engine power), location, and odometer.

RECEIPTS

All Receipt data related to identified users are deleted when their associated expense reports are deleted.

Receipt data includes but is not limited to:

- Attached receipt images.
- All electronic receipt details from vendors that use our supported electronic receipt schemas.

REQUEST

All Request data related to identified users are deleted when their associated expense reports are deleted. The Request details include but are not limited to:

- Request Header content, Request Entry content, Report Entry reference, Cash Advance reference, Itinerary.
- Agency Proposal, Segment details.

TRAVEL ALLOWANCE

All Travel Allowance data related to identified users are deleted when their associated expense reports are deleted or if there is an unused Travel Allowance.

Travel Allowances contain but are not limited to:

- Company ID, User ID, Dates/times, departure and arrival location, addresses, itinerary ID, description, lodging details, daily allowance details.

NOTE: If you use the Budget feature together with Central Reconciliation, refer to the *Shared: Budget Setup Guide* for more information.

Feature Benefits

The Data Retention feature provides the following functionality:

- Enables a company to set a specific amount of calendar time after which data such as old user profiles, itineraries, credit card account information, and expense reports is removed.
- Enables you to place a hold on a specific user whose data will be excluded by this feature accommodating the necessity or desire to retain specific users' older data.

! **IMPORTANT:** The maximum number of users you can put on hold is 1000. HOLD feature work cannot be guaranteed for users that exceed the limit of 1000. If you require more than 1000 users to be placed on HOLD, open an SAP Concur service ticket.

- Provides a high-level summary of events to monitor data retention activities.

This document describes how to enable, configure, and manage the Data Retention feature for Concur services.

Terminology

This table describes the terminology used for the Data Retention feature.

Term	Description
Data Retention	The name of the Concur feature intended to help clients remove personal data.
personal data	Any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier.
Sensitive Data [page]	A setting of this feature for a subset of personal data that is not needed beyond the termination of an employee and therefore has an expedited retention period. For example, a user's passport number, emergency contact information, travel preferences, driver's license number, and US Social Security Number.
removed [data]	The single term that refers to the anonymization, deletion, or obfuscation of data by the Data Retention feature. Also known as purged or deleted data.
obfuscated [data]	Data that has been rendered unintelligible and thereby useless for identifying a specific person. This is also known as removed [data].
anonymized [data]	Data that has been rendered anonymous and thereby useless for identifying a specific person. This is also known as removed [data].
activated	When the Data Retention configuration takes effect. If no admin intervenes, a new or updated retention period is activated automatically after the mandatory 72-hour waiting period.
anchor date	The date that the Data Retention feature uses to determine age of a piece of data. The age is calculated as a delta from the current date.
Hold User	A button of this feature for enabling the functionality that exempts a user's data from being removed by the Data Retention feature. ! IMPORTANT! The maximum number of users you can put on hold is 1000. HOLD feature work cannot be guaranteed for users that exceed the limit of 1000. If you require more than 1000 users to be placed on HOLD, open an SAP Concur service ticket.

Data Retention Roles

For Expense, Request, and Invoice, in Standard Edition, the existing admin roles have been granted the permission to administer (set up and edit) the Data Retention configuration. For Travel, in Standard Edition, a new role was created.

Concur Service	Role	Description
Expense (includes Request)	Can Administer (existing role)	Can view and access the Data Retention link on the Tools page and will receive a 72-hour confirmation email of their configuration changes.
Invoice	Is Invoice Admin (existing role)	Can view and access the Data Retention link on the Tools page and will receive a 72-hour confirmation email of their configuration changes.
Travel	Is Data Retention Admin (new role)	Can view and access the Data Retention link on the Tools page and will receive a 72-hour confirmation email of their configuration changes. NOTE: For Standard Travel, the <i>Is Data Retention Admin</i> permission can only be selected (viewed) by Concur Admin. SAP Concur must select it for clients.

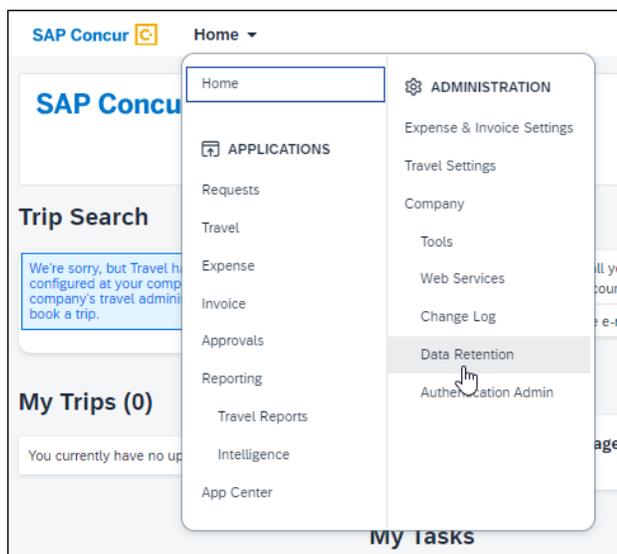


For more information, refer to the *Shared: Users Guide*.

What the Admin Sees

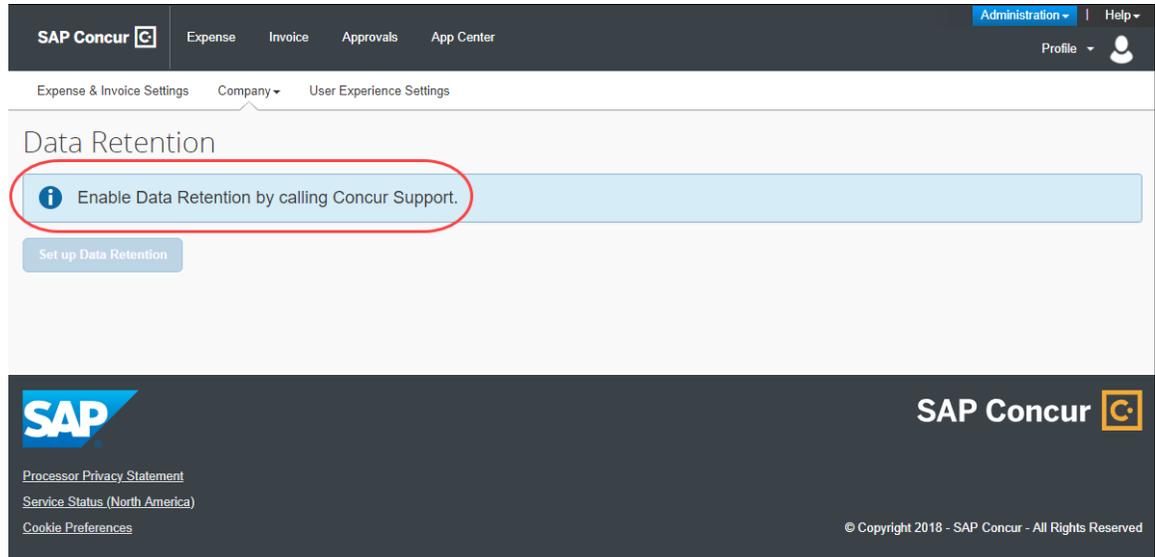
What an admin sees depends on their roles and whether SAP Concur has enabled this feature for their company.

When the feature is enabled by SAP Concur, an admin with the required roles, sees **Data Retention** in the **Administration** menu.



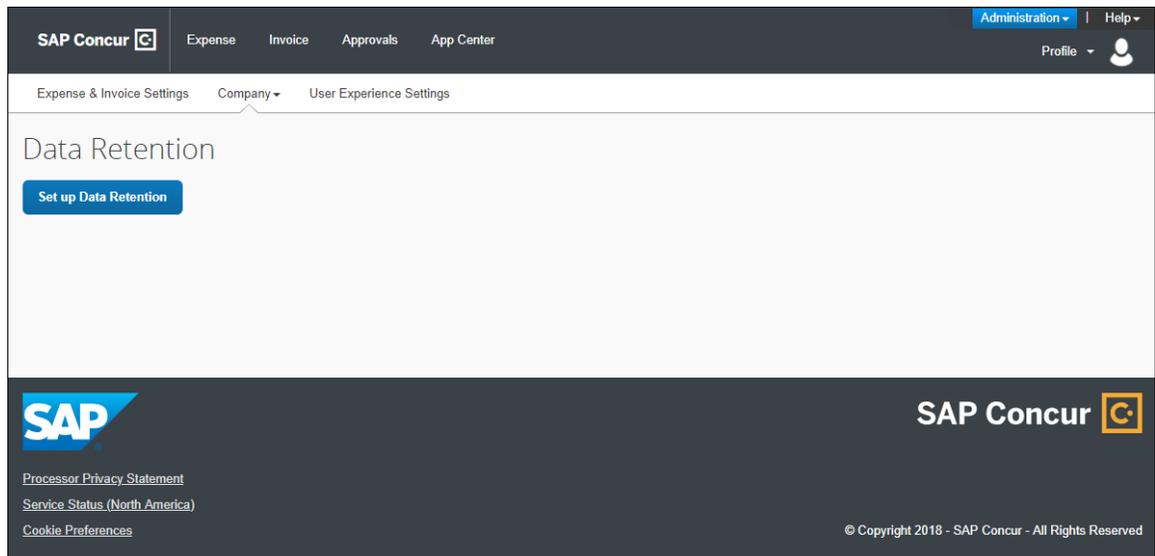
ENABLING THE DATA RETENTION FEATURE

To be allowed to set up the Data Retention feature, a user must contact SAP Concur. Only SAP Concur can enable the feature.



SETTING UP THE DATA RETENTION FEATURE

Once enabled by SAP Concur, a Data Retention Administrator can access the set up wizard and configure this feature.



Section 3: How It Works

The Data Retention feature is disabled by default for all clients. If a client contacts SAP Concur and requests this feature, SAP Concur support will enable the feature so that a client admin can begin configuring it. A client admin will set a length of time for data to be retained. The system gives that client admin 72 hours to edit the Data Retention configuration. After the 72-hour mandatory waiting period, when Concur detects data that is older than the time configured, the removal process begins. The monitor tab within the Data Retention product will provide high-level, summary information about data that is removed.

Please Note the Following

Creating a Company Data Retention Plan

SAP Concur strongly recommends that clients have a company data retention plan that includes communicating necessary details about the company's data retention policy to employees and those who depend on reports generated from the SAP Concur solution. SAP Concur is unable to advise clients on specific time ranges for setting the years of retention. SAP Concur clients are responsible for evaluating their company's legal and statutory needs and configuring the Data Retention feature to meet those needs.

Factoring Your Time Range to Retain or Remove Credit Card Data

The Data Retention feature provides flexibility to remove credit card numbers from a client's Concur Expense database on demand. This should be factored into any determination of the appropriate time ranges chosen to retain this data.

NOTE: The records in the Concur Pay system are not affected by the Data Retention feature.

For Clients Who Use the Employee Import Feature

Clients who use the Employee Import feature must ensure that sensitive user data removed by the Data Retention feature is also removed from their Employee Import source files.

! **IMPORTANT:** To prevent a user's sensitive data from being re-imported after it has been removed from SAP Concur solutions, it is the responsibility of the client to remove or otherwise exclude the information from any Employee Import source files so that data removed by the Data Retention feature is not re-imported into SAP Concur through the Employee Import feature. For more detailed information, refer to the FAQ section of this document.

Overview Steps

▶ **How to use the Data Retention feature**

1. A client contacts SAP Concur with a desire to use the feature and provides login IDs of users who need Data Retention Administrator permission.

! **IMPORTANT:** Before enabling the Data Retention feature, ensure that all unassigned transactions older than 23 months have been processed. After enabling the Data Retention feature, unassigned transactions should be routinely monitored using Reporting. For more information, refer to *The 23-Month Filter* section of this document.

2. SAP Concur support enables the feature and grants Data Retention Administrator permission to users specified by the client.
3. A client admin configures the data retention periods using the setup wizard.
4. The system emails a confirmation of the change and begins a 72-hour mandatory waiting period during which changes can be made before removals begin.

NOTE: There will always be at least 72 hours between when the data retention periods are setup or changed and they become activated.

5. After the 72-hour mandatory waiting period is over, the system begins checking each day for data that is old enough to be impacted by the retention periods. If old data is found, the system begins removes it.
6. A client admin can view summary information about the purge from the monitor.
7. When needed, a client admin modifies the data retention periods.
8. When needed, a client admin holds (exempts from removal) the data of a specific user.



For more information, refer to the *Shared: Data Retention User Guide*.

FAQs

Q: For which services can Data Retention be configured?

A: Data Retention can be configured independently for all core services: Travel, Expense, Invoice, and Request. In addition, there are separate settings for Sensitive Data.

NOTE: While each service can have its own settings, **all services must be configured**. It is not possible to turn on Data Retention for only Expense or for only Travel.

Q: What is the shortest and longest length of time that can be configured for Data Retention?

A: For core services, such as Expense and Travel, no shorter than two (2) years and no longer than 20 years can be configured. For Sensitive Data, no shorter than one (1) month and no longer than 12 months can be configured.

Q: Can Data Retention be configured by country?

A: Data Retention for Travel can be set by configuration. Data Retention for Expense can be set by policy. To set retention periods by country, each country will need its own configuration and policy.

Q: If one person creates an expense report for another person, or arranges travel for another person, which user's Data Retention Policy settings will be used?

A: When a user creates data for another user the Data Retention settings will be applied based on the user who is assigned to the data, the owner of the data, and **not** the user who created the data.

Q: How does the SAP Concur Employee Import process affect Data Retention?

A: Clients who use the Employee Import feature must ensure that user data removed by the Data Retention feature is also removed from their Employee Import source files.

! IMPORTANT: To prevent a user's sensitive data from being re-imported after it has been removed from SAP Concur solutions, it is the responsibility of the client to remove or otherwise exclude the information from any Employee Import source files so that data removed by the Data Retention feature is not re-imported into SAP Concur through the Employee Import feature.

If a user is included in an Employee Import (data record layout 300 or 305) and the sensitive data retention period for that user expires so that the user's sensitive data is removed from SAP Concur solutions, the user's sensitive data could be re-imported and repopulated in SAP Concur with the next Employee Import. After it is reimported, SAP Concur will not remove this sensitive data, since the client has chosen to re-import it. The client must take manual action if this occurs.

Time Measurement

The Data Retention feature applies to certain kinds of data. For those kinds of data, the feature determines the age of the data. The age is calculated based on the date of the data compared to today's date. If the age is determined to be older than the retention period that was selected when the Data Retention periods were configured, then that data is removed.

Determining the Age of the Data

The Data Retention feature calculates the age of data to determine if that data is old enough to be removed from the system.

Kind of Data	Anchor Date
Users / Profiles	<p>A user's User Administration page data does not begin to age until the user is designated as inactive.</p> <p>A user's User Administration page data and other profile data are calculated as the difference between the user's inactive date and today.</p> <p>Note: User data is removed or anonymized in two intervals:</p> <ul style="list-style-type: none"> Profile Purge Policy interval 1: This timeframe is defined by the customer and can be 1 - 12 months. Once this interval elapses, the user's data that has no bearing on transactional data will be deleted or anonymized. Examples include a user's email address, passport number, emergency contact information, travel preferences, driver's license number, and US Social Security Number. <p>Profile Purge Policy interval 2: Once the following three criteria are met the user's remaining profile data will be removed or anonymized: 1) the user is inactive; 2) the longest retention period is reached; and 3) if there is no hold on the user's data.</p> <p>This process is also consistent with Users that have never incurred transaction activity from the SAP Concur product. For example, assume the Profile Purge policy (interval 1) is set at 12 months and the longest Data Retention Policy is 10 years. Also assume a user is not on hold and they are inactivated today. The user's profile data (mentioned above for interval 1) will be removed or anonymized 12 months and one day after the inactive date value. The user's remaining profile data will be removed or anonymized 10 years and one day after the inactive date value. The best practice is to not back-date the termination date value to a value that is before the user's last transaction's anchor date. For example, if a user's last expense report was Sent for Payment on January 8, 2024, the user's termination date should not be prior to January 8, 2024.</p> <hr/> <p>! IMPORTANT: For clients who use both Employee Import and Data Retention, it is the responsibility of the client to remove employee data from the Employee Import source files when user data is removed from the SAP Concur system by the Data Retention feature. For more detailed information, refer to the FAQ section of this document.</p> <hr/> <p>A User's other profile data is managed the same as the user's User Administration page data.</p>
Itineraries	The age of an itinerary is calculated as the difference between its creation date and today.
Expense reports	The age of an expense report is calculated as the difference between its paid date and today. If an Expense report has no paid date, (for example, it was not submitted) then the data retention feature uses the creation date.

Section 3: How It Works

Kind of Data	Anchor Date
Authorization requests	When assigned to an Expense report, the age is determined by the age of the report, (for example, the authorization requests are not deleted until the report is deleted.) NOTE: Legacy authorization requests are only removed if they were assigned to an expense report.
Cash advances	When assigned to an Expense report, the age is determined by the age of the report, (for example, the cash advances are not deleted until the report is deleted.) When a cash advance is not assigned to a report, the age of the cash advance is calculated as the difference between the request date and today.
Credit card transactions	When assigned to an Expense report, the age is determined by the age of the report, (for example, the credit card transactions are not deleted until the report is deleted.) When a credit card transaction is not assigned to a report, the age of the credit card transaction is calculated as the difference between the posted date and today.
Credit Card Accounts	The age of an account is calculated as the difference between the date of the most recent card transaction imported for the account and today. If there have been no transactions imported for an account, the age of that account is calculated as the difference between its creation date and today.
E-Receipts	When assigned to an Expense report, the age is determined by the age of the report, (for example, the e-receipts are not deleted until the report is deleted.)
Concur mobile app entries	When assigned to an Expense report, the age is determined by the age of the report, (for example, the Concur mobile app entries are not deleted till the report is deleted.) When a mobile entry is not assigned to a report, the age of the mobile entry is calculated as the difference between the transaction date and today.
Japan Public Transport (JPT) route information	When assigned to an Expense report, the age is determined by the age of the report (for example, the JPT route information is not deleted until the report is deleted.)
Invoices	The age of the request is based on the date the invoice was created in the system.
Purchase requests	The age of a purchase request is based on its last modified date of the request.
Purchase orders	The age of a purchase order is based on the creation date of the PO. Note: The PO and Goods Receipts related to the PO will be removed along with the PO when they are beyond the retention period, and all the related records to the PO such as Invoices and Purchase requests have also been removed and are beyond the retention period.
Requests	The age of a request is calculated as the difference between its close date and today. If the request is not closed, then the request creation date is used to determine its age.

EXAMPLE

If a submitted request has a close date of December 31, 2017, then on December 31, 2019, that request is two years old. If the Data Retention periods are configured to delete Request data that is older than two years old, then the earliest that this request will be deleted is January 1, 2020, but may be deleted after this date depending on the age of any linked Expense Report, and any accompanying Cash Advances.

Retention Periods

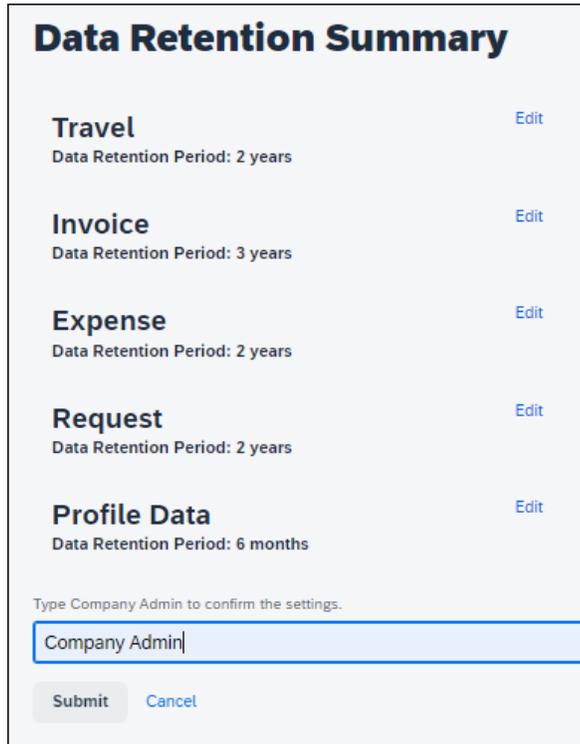
In the Data Retention setup wizard, the list of years to choose from are not calendar years. Rather, the years can be thought of as ages. The feature is **not** designed to delete all data from a calendar year, such as all data from the year 2001. The feature **is** designed to delete data each day, day after day, that has reached a certain age, such as 3 years old.

EXAMPLE

On June 1, 2018, a client admin uses the Data Retention setup wizard to configure or edit the company's Data Retention periods. For each service, such as Expense or Travel, the client admin enters a retention period of 3 years and clicks **Submit** to save the configuration. After the 72-hours waiting period, the system begins a daily check for old data. If no other changes are made to the configuration, on June 4, 2018, the system begins removing data that is equal to or more than 3 years and one day old. In this example, an expense report dated June 4, 2015 (or earlier) will be removed, but an expense report dated June 5, 2015 will not be removed until the next day.

72-Hour Activation Waiting Period

As a safeguard to undesired updates to the Data Retention periods, a 72-hour waiting period is required before the system activates a new or changed configuration. Each time the **Submit** button is clicked, the 72-hour confirmation email for any configuration changes is triggered.



The screenshot shows a 'Data Retention Summary' page with a list of categories and their retention periods. Each category has an 'Edit' link to its right. At the bottom, there is a confirmation step where the user must type 'Company Admin' into a text field, followed by 'Submit' and 'Cancel' buttons.

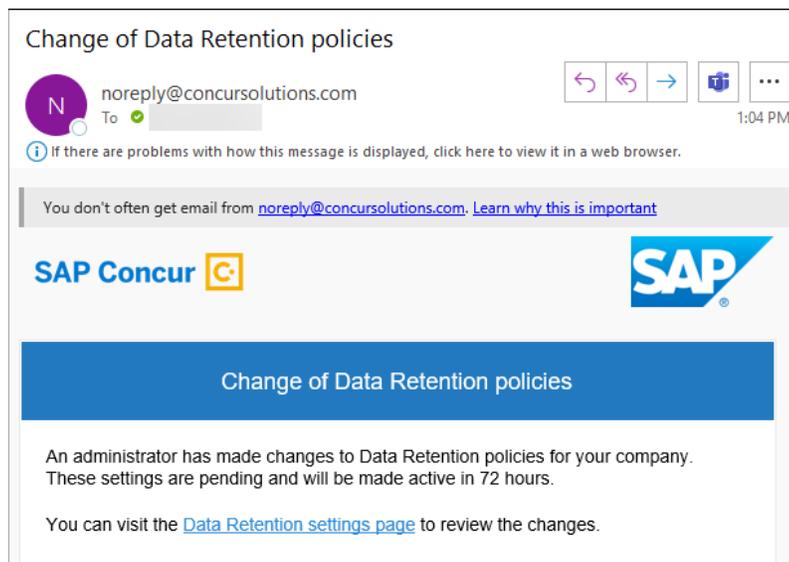
Category	Data Retention Period	Action
Travel	2 years	Edit
Invoice	3 years	Edit
Expense	2 years	Edit
Request	2 years	Edit
Profile Data	6 months	Edit

Type Company Admin to confirm the settings.

Company Admin

Submit Cancel

Each time the **Submit** button is clicked, the 72-hour confirmation email for any configuration changes is triggered.



The 23-Month Filter

A 23-month filter is included with the Data Retention feature and will automatically filter older transactions. The transactions are not recoverable. The filter impacts the following areas:

- Available Expenses
- View (unassigned) transactions in Expense (including statement periods older than 23 months)
- Unassigned Cash Advances

NOTE: The filter is only available to clients who enable the Data Retention feature.

The 23-month time is not configurable and cannot be turned off.

! **IMPORTANT:** Before enabling the Data Retention feature, ensure that all unassigned transactions older than 23 months have been processed. After enabling the Data Retention feature, unassigned transactions should be routinely monitored using Reporting.

This filter reduces the accumulation of unprocessed transactions over time and supports the Data Retention feature.

Unusual Scenarios

Request

The following scenarios are only possible for Request clients who use Data Retention but choose **not** to use the recommended auto-close option (available for Professional Edition clients and forced to ON with a setting of 90 days for Standard Edition clients.)

LATE EXPENSE REPORTS

In some countries, Expense reports may be submitted very late (e.g. in France, per legislation, up to 5 years after the spend occurred). If a user has an approved Request and an Expense report linked to this Request and due to the Data Retention feature configuration, this Expense report is removed, it would then be possible for the user to create an additional Expense report based on this same Request.

! **IMPORTANT:** To prevent this scenario, SAP Concur recommends that you use the auto-close option. Otherwise, to minimize the possibility of this scenario, SAP Concur recommends that the Data Retention feature be configured with the same number of years for Expense and for Request.

TWO EXPENSE REPORTS FOR ONE REQUEST

If a Request is linked to two Expense reports and one Expense report expires, the Request amount will no longer be valid, and it is possible for the user to modify the remaining Expense reported to double claim already reimbursed funds.

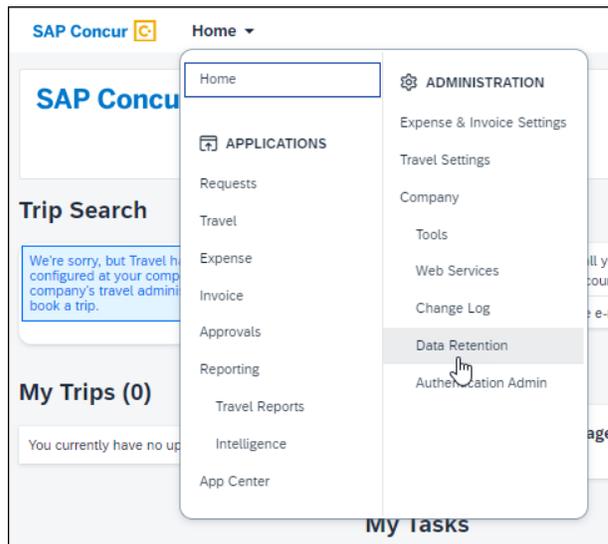
! **IMPORTANT:** To prevent this scenario, SAP Concur recommends that you use the auto-close option. Otherwise, to minimize the possibility of this scenario, SAP Concur recommends that the Data Retention feature be configured with the same number of years for Expense and for Request.

Section 4: Administrator Experience

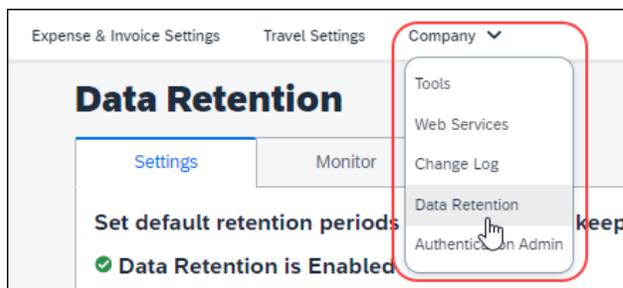
If enabled by SAP Concur, on the **Company** list, the client admin will see a **Data Retention** link.

► **To access Data Retention**

1. Log in as an admin or in the case of Travel, a data retention admin.
2. Click **Data Retention** in the **Administration** menu.



Data Retention is also available in the **Company** list.

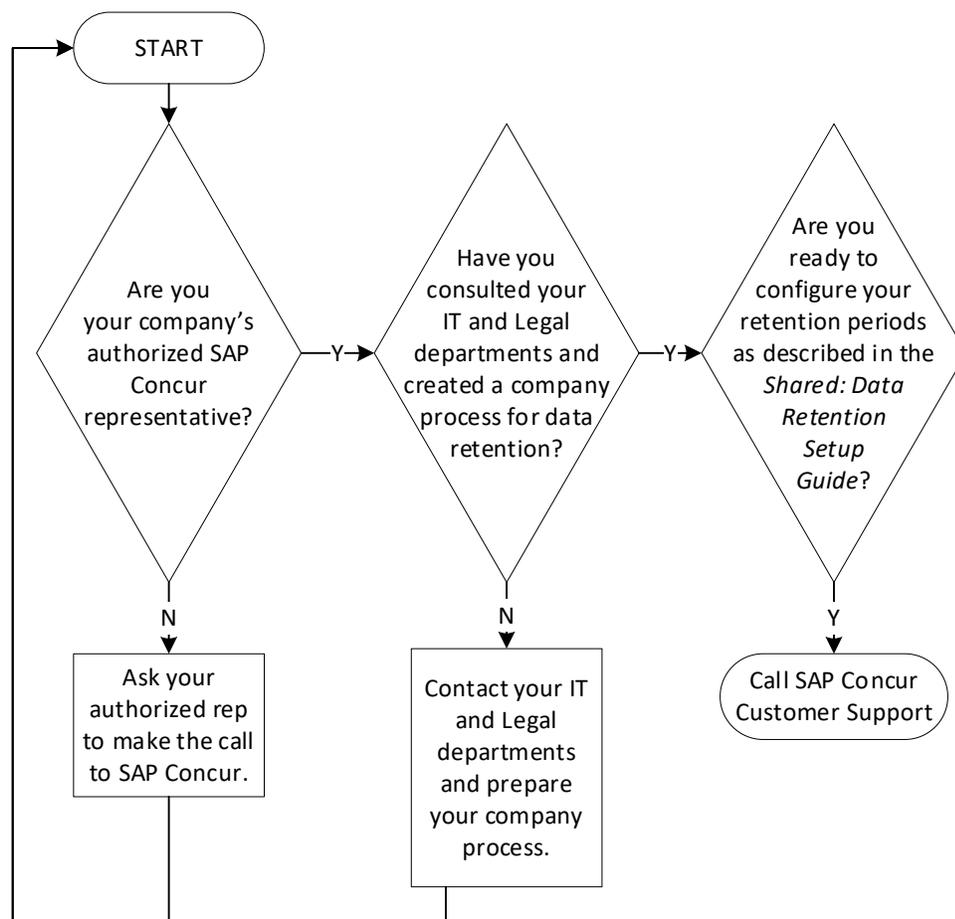


Section 5: Activation

Only SAP Concur can enable this feature so that you may configure it for your company.

! IMPORTANT:

- Data Retention cannot be turned off once enabled.
- It is not possible to turn on Data Retention for only some parts of a company; this is a company-wide feature.
- The 23-month filter applies immediately upon feature enablement, regardless of whether Data Retention settings have been configured and saved.



! Before enabling the Data Retention feature, ensure that all unassigned transactions older than 23 months have been processed.

Section 6: Configuration

Once activated, this feature can be accessed from the **Administration** or **Company** list.

Overview

The client admin uses the following process to configure the Data Retention feature for the applicable SAP Concur products/services:

1. Select a default retention period in years for Travel and optionally select retention periods for Travel configuration groups.
2. Select a default retention period in years for Expense and optionally select retention periods for Expense policy groups.
3. Select a default retention period in years for Invoice and optionally select retention periods for Invoice policy groups.
4. Select a default retention period in years for Request and optionally select retention periods for Request policy groups.
5. Select the retention period in months for Sensitive Data.
6. (Optional) Place holds on specific users so they will be exempt from the data retention periods.

Users who Change Policy Groups

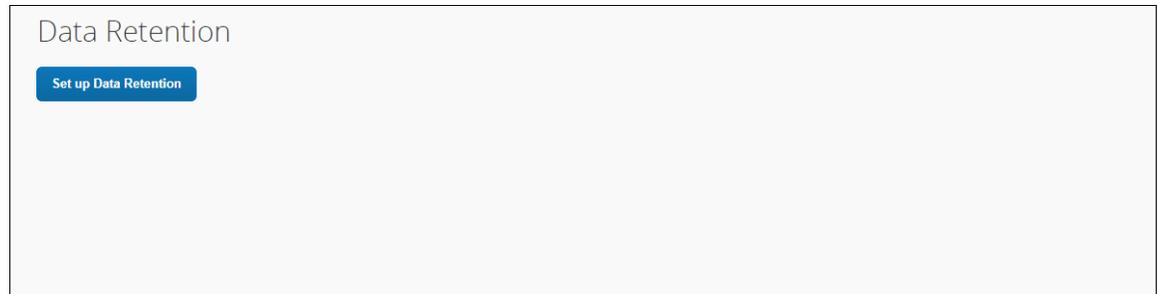
The history of policy group memberships is taken into consideration by the Data Retention feature. A user who changes policy group may have different portions of their data impacted by different retention periods.

EXAMPLE

Pat was in Germany and was part of the German policy group and submitted reports there. The Expense data retention period for users with the Germany policy is 10 years. Pat has transferred to the US and switches policy groups. The Expense data retention period for users with the US policy is 7 years. Some of Pat's expense reports (the new ones) are impacted by the 7-year retention period while Pat's older reports, submitted in Germany, are impacted by the 10-year retention period. In effect, Pat's oldest reports, from Germany, may be retained longer than the reports Pat submitted right after transferring to the US, even though the US expense reports are newer. Pat's 8-year-old expense report that was submitted while they were a member of the US policy group will be removed by the Data Retention configuration before Pat's 9-year-old expense report that was submitted while Pat was a member of the Germany policy group.

Access the Data Retention Pages

After SAP Concur support enables the feature, clients will see the available **Set up Data Retention** button.

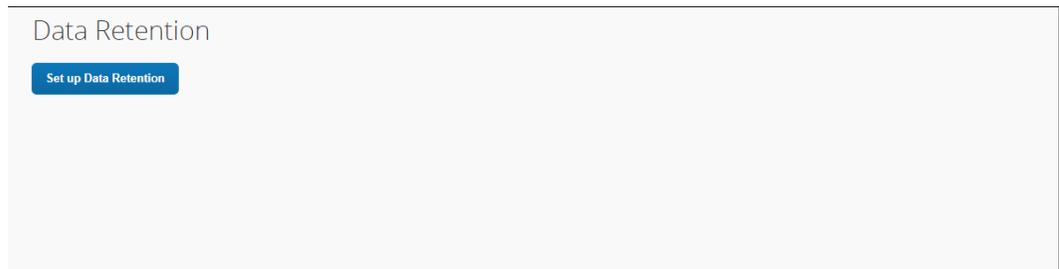


To access the **Data Retention** configuration pages, click **Administration > Company > Data Retention**. The **Data Retention** page appears.

Configure the Data Retention Periods

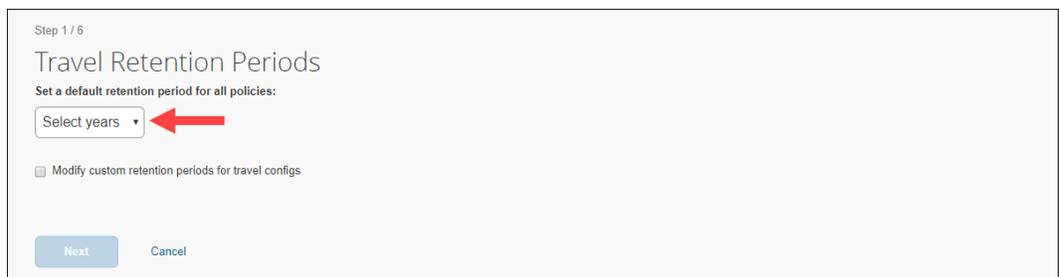
► *To configure data retention:*

1. On the **Data Retention** page, click **Set up Data Retention**.



NOTE: These steps represent the experience of a client admin whose company uses all the products supported by the Data Retention feature. For some client admins, this wizard may present fewer pages/steps.

2. On the **Travel Retention Periods** step of the Data Retention wizard, from the **Select years** list, select the desired number of years after which data will be removed.



Section 6: Configuration

3. Select **Modify custom retention periods for travel configs.**

! **IMPORTANT!** The retention periods for configs override the default retention period.

4. Select a config name and use the **Edit Years** list to populate the **Years** column of the grid.

Step 1 / 6

Travel Retention Periods

Set a default retention period for all policies:

3 years

Modify custom retention periods for travel configs

Edit Years

Config Name	Years
<input type="checkbox"/> CommaSavvy AUT Property Per Diem	3
<input type="checkbox"/> CommaSavvy AUT PBL	3
<input checked="" type="checkbox"/> CommaSavvy AUT Location Per Diem	3

Next Cancel

5. Repeat the previous step until each config has been assigned a number of years.

6. Click **Next**.

7. On the **Invoice Retention Periods** page of the Data Retention wizard, from the **Select years** list, select the desired number of years after which data will be removed.

Step 2 / 6

Invoice Retention Periods

Set a default retention period for all policies:

Select years

Modify custom retention periods for Invoice policies

Previous **Next** Cancel

8. Select **Modify custom retention periods for Invoice policies.**

! **IMPORTANT:** The retention periods for polices override the default retention period.

9. Select a policy and use the **Edit Years** list to populate the **Years** column of the grid.
10. Repeat the previous step until each policy has been assigned a number of years.
11. Click **Next**.
12. On the **Expense Retention Periods** page of the Data Retention wizard, from the **Select years** list, select the desired number of years after which data will be removed.

13. Select **Modify custom retention periods for Expense policies**.

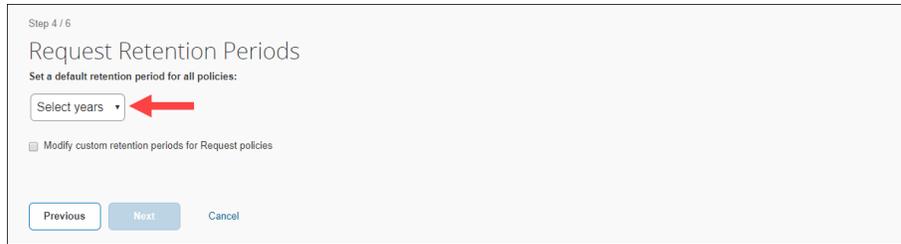
! **IMPORTANT:** The retention periods for polices override default retention periods.

14. Select a policy. Use the **Edit Years** list to populate the **Years** column of the grid.
15. Repeat the previous step until each policy has been assigned a number of years.
16. Click **Next**.
17. On the **Request** page of the Data Retention wizard, from the **Select years** list, select the desired number of years after which data will be removed.

NOTE: It is a best practice to set your Request retention period(s) to match the number of years you set for Expense. It is very important to do this because, if the Concur Request retention policy is set to a shorter period of time than Concur Expense, the requests would be deleted first, and clients would lose the request pre-authorization information for the expense reports associated with the deleted requests.

Another best practice for Request clients who use Data Retention is to use the auto-close option (available for Professional Edition clients and forced to ON with a setting of 90 days for Standard Edition clients), or be diligent about manually closing requests. These strategies help avoid possible orphaned requests that may remain in the system after the corresponding expense report has been removed.

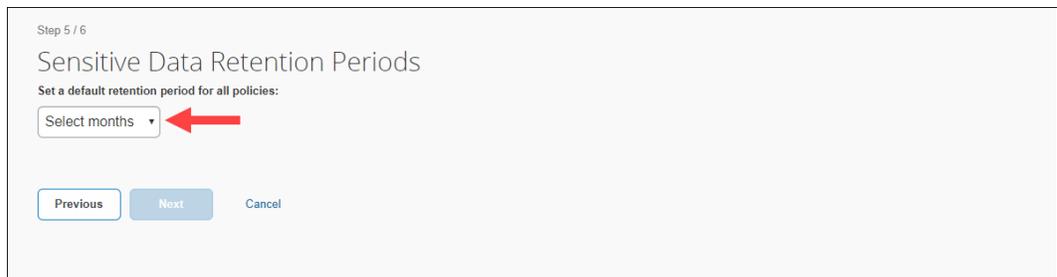
Section 6: Configuration



18. Select **Modify custom retention periods for Request policies**.

! **IMPORTANT:** The retention period for polices overrides the default retention period.

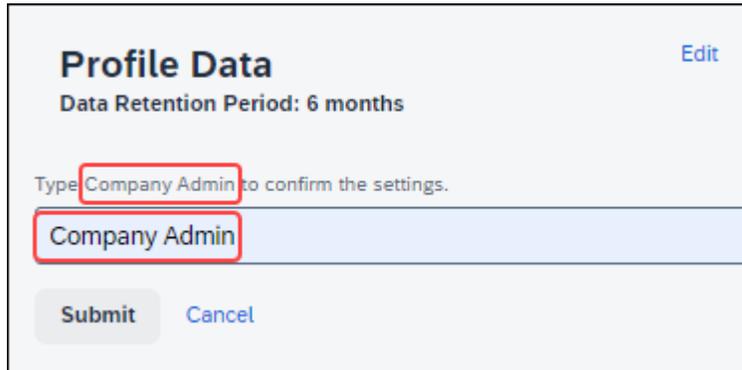
19. Select a policy and use the **Edit Years** list to populate the **Years** column of the grid.
20. Repeat the previous step until each policy has been assigned a number of years.
21. Click **Next**.
22. On the **Sensitive Data** page of the Data Retention wizard, from the **Select months** list, select the desired number of months after which data will be removed.



! **IMPORTANT:** For clients who use both Employee Import and Data Retention, it is the responsibility of the client to remove employee data from the Employee Import source files when user data is removed from the SAP Concur system by the Data Retention feature. For more detailed information, refer to the FAQ section of this document.

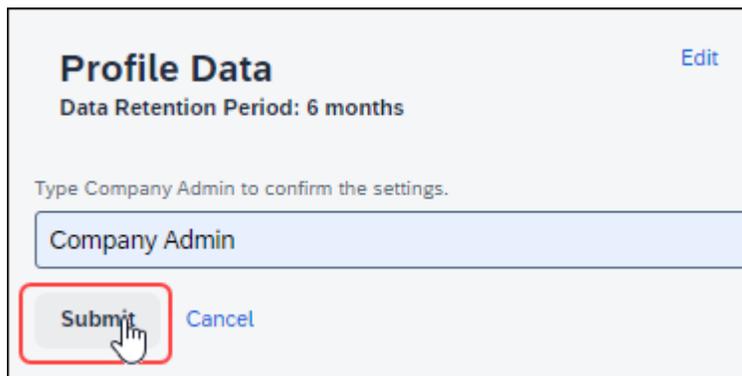
23. Click **Next**.

24. On the bottom of the **Data Retention Summary** page, type your name as it appears.



The screenshot shows a form titled "Profile Data" with a blue "Edit" link in the top right corner. Below the title, it says "Data Retention Period: 6 months". The main instruction is "Type Company Admin to confirm the settings." Below this instruction is a text input field containing "Company Admin". At the bottom of the form are two buttons: "Submit" and "Cancel".

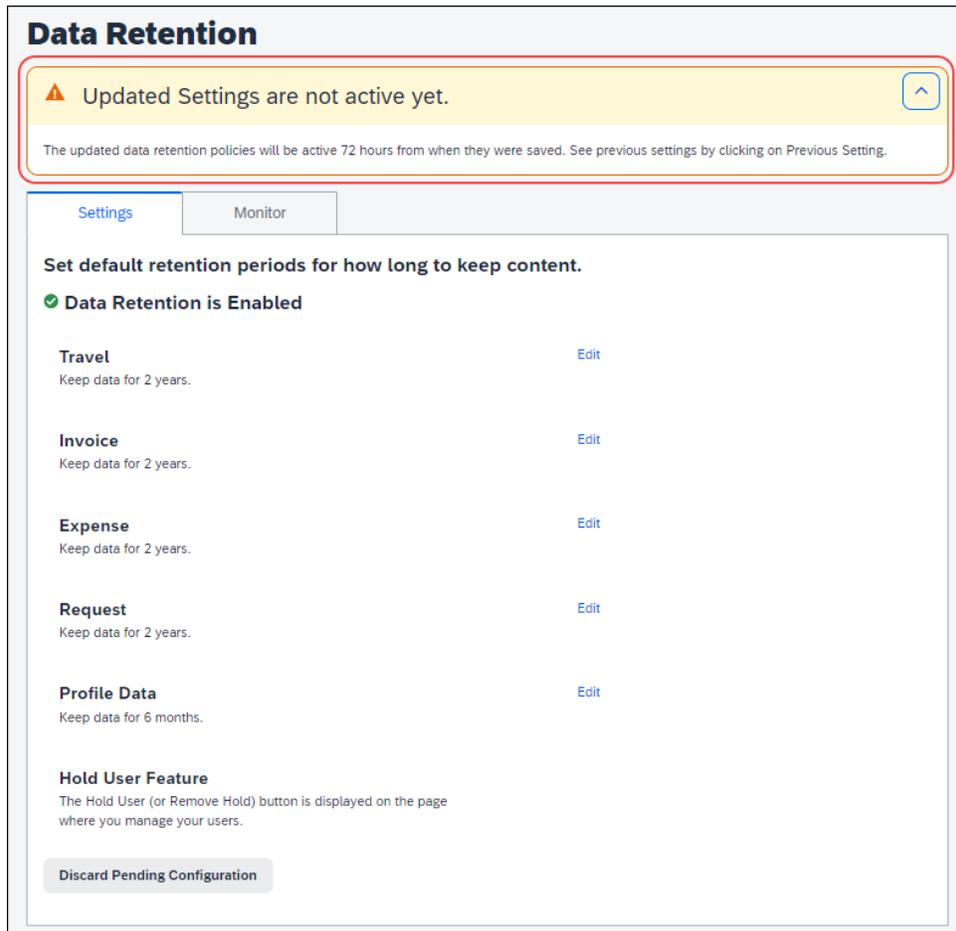
25. Click **Submit**. The retention periods are saved, the mandatory 72-hour waiting period begins, and you will receive a confirmation email.



This screenshot is identical to the previous one, but with a red box around the "Submit" button and a mouse cursor pointing at it, indicating the next step in the process.

Section 6: Configuration

26. Verify that the mandatory 72-hour waiting period has started.



Data Retention

⚠ Updated Settings are not active yet. ⬆

The updated data retention policies will be active 72 hours from when they were saved. See previous settings by clicking on Previous Setting.

[Settings](#) [Monitor](#)

Set default retention periods for how long to keep content.

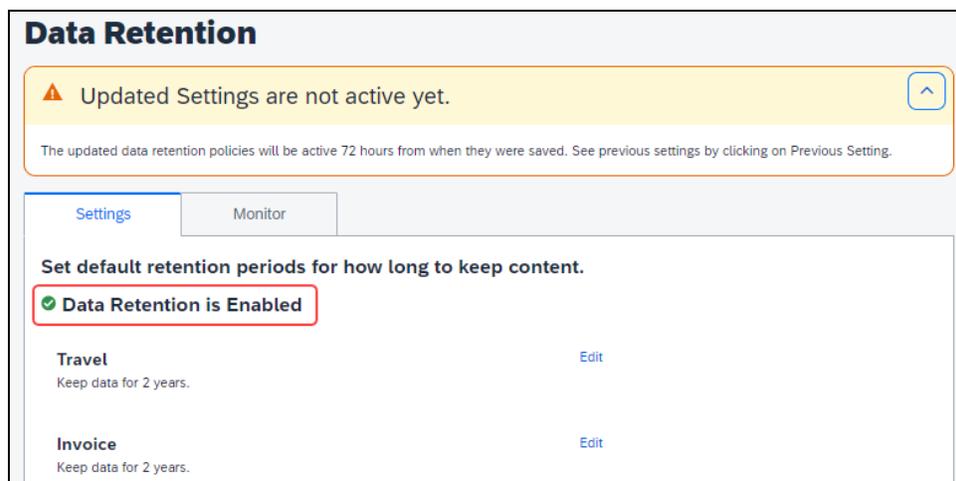
✔ **Data Retention is Enabled**

Travel Keep data for 2 years.	Edit
Invoice Keep data for 2 years.	Edit
Expense Keep data for 2 years.	Edit
Request Keep data for 2 years.	Edit
Profile Data Keep data for 6 months.	Edit

Hold User Feature
The Hold User (or Remove Hold) button is displayed on the page where you manage your users.

[Discard Pending Configuration](#)

27. Verify that the Data Retention feature is enabled.



Data Retention

⚠ Updated Settings are not active yet. ⬆

The updated data retention policies will be active 72 hours from when they were saved. See previous settings by clicking on Previous Setting.

[Settings](#) [Monitor](#)

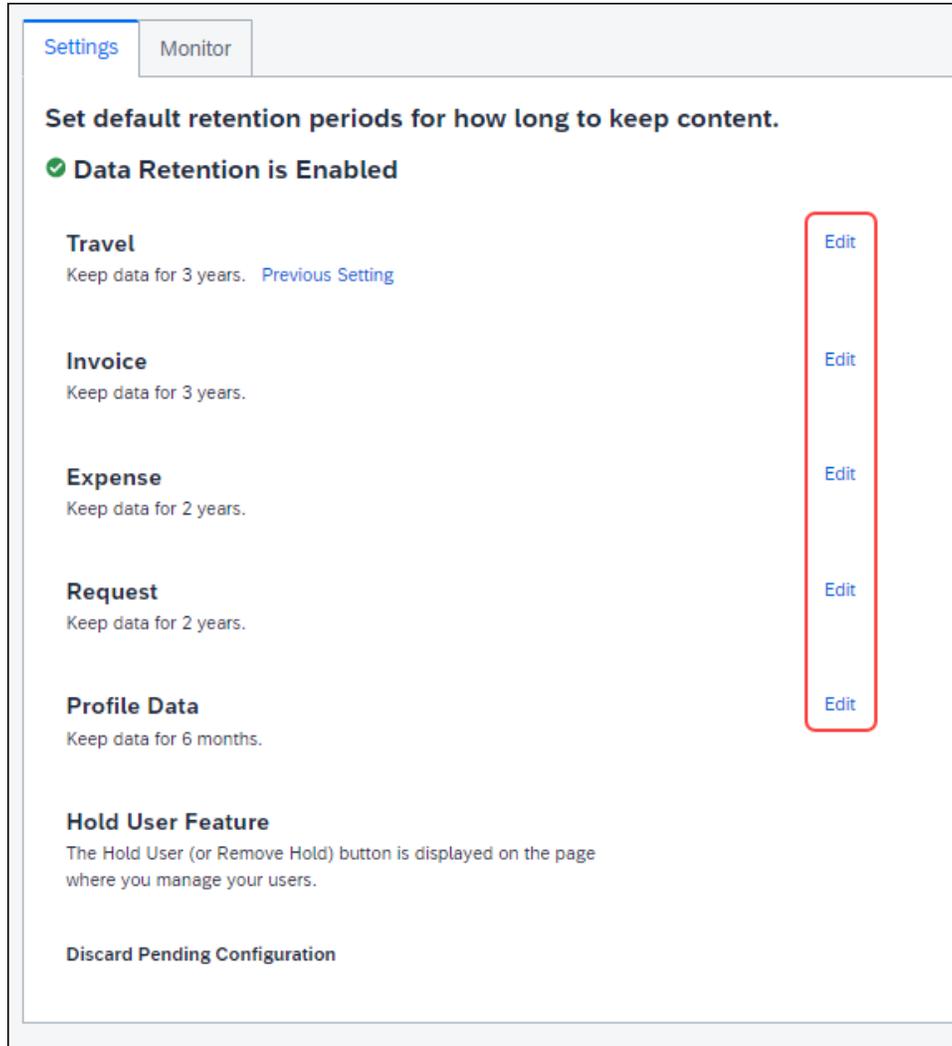
Set default retention periods for how long to keep content.

✔ **Data Retention is Enabled**

Travel Keep data for 2 years.	Edit
Invoice Keep data for 2 years.	Edit

Edit the Data Retention Periods

After the initial configuration is complete, the **Settings** tab of the **Data Retention** page has **Edit** links for changing the configuration. Click **Edit** to return to the wizard page where you can edit settings.



Section 7: Monitoring

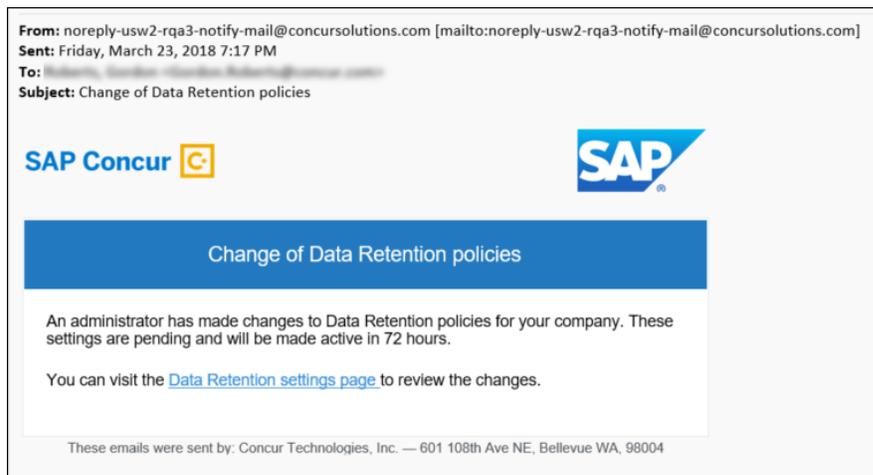
Configuration Changes

When configuration changes are made, a cooling-off period of 72 hours allows the Data Retention Administrator to discard pending configuration changes.

Email Confirmation of Pending Changes

Clicking **Submit** for changes to the configuration, triggers the system to send an email confirmation to the Data Retention Administrator that changes are pending. This allows time for the changes to be discarded or further edited before the changes take effect.

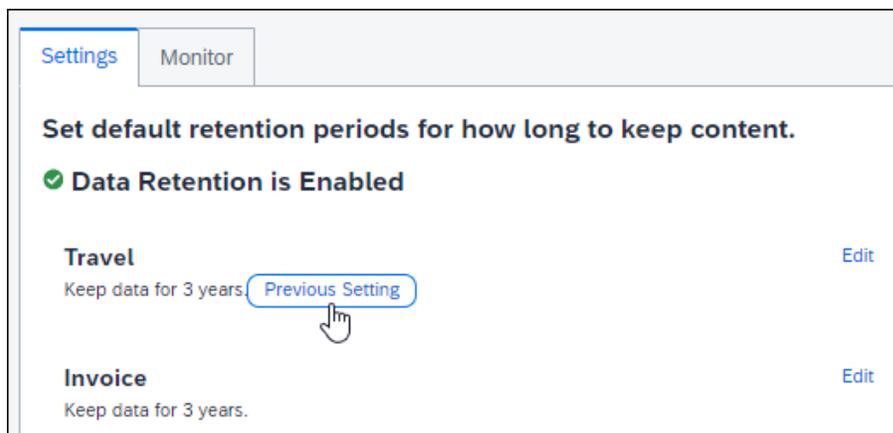
EXAMPLE CONFIRMATION EMAIL



View Pending Changes

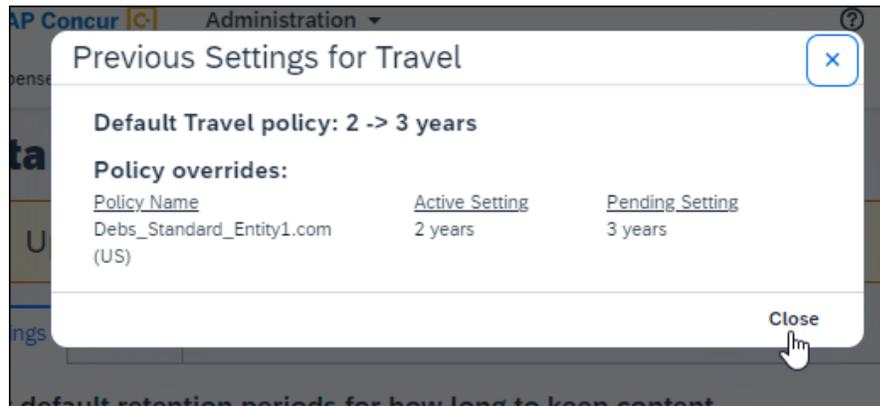
▶ To view pending configuration changes

1. On the **Company Administration** page, click **Data Retention**.
2. Click **Previous Settings**.



NOTE: The page may display more than one **Previous Setting** link, each with unique information.

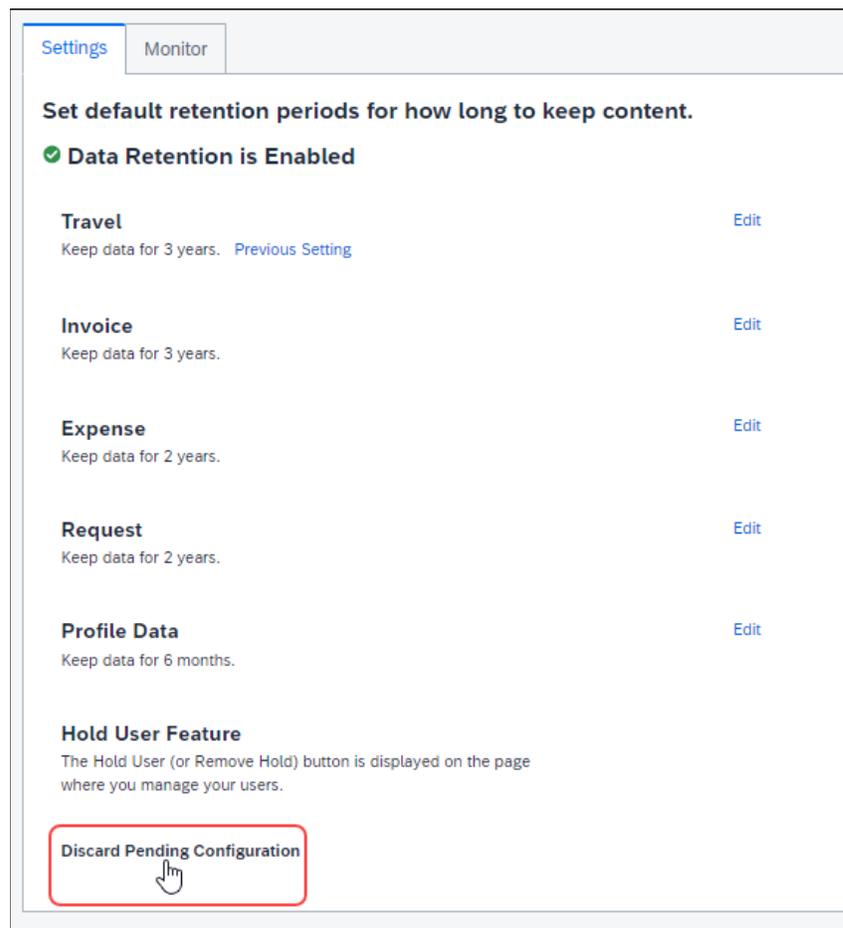
3. Click **Close**.



Discard Pending Changes

- ▶ **To discard pending configuration changes**

4. On the **Company Administration** page, click **Data Retention**.
5. Click **Discard Pending Configuration**.



Removed Data

Successfully removed records are indicated by count on the **Monitor** tab.

The screenshot shows the 'Data Retention' interface with the 'Monitor' tab selected. A yellow warning banner at the top states 'Updated Settings are not active yet.' Below this, the 'Monitor' tab is active, and a green checkmark indicates 'Data Retention is Enabled'. The 'Start Date' is 03/08/2018 and the 'End Date' is 03/15/2018. A table displays the following data:

Date	Resource	Delete Count
15-Mar-2018	UserProfile	7

When the feature has been configured, but no records have been removed yet, the **Monitor** tab indicates that the feature is enabled, but no data has been deleted.

The screenshot shows the 'Data Retention' interface with the 'Monitor' tab selected. A green checkmark indicates 'Data Retention is Enabled'. The table below is empty, and a red-bordered box highlights the text 'No Data Has Been Deleted' in the center of the table area.

Date	Resource	Delete Count
No Data Has Been Deleted		

NOTE: The length of time Concur requires to complete the removal process varies based on factors such as time of day, amount of data, and location (including backups) of data, and managed holds. Use the **Monitor** tab of the **Data Retention** page to view a summary of items that have been removed.

Resources

The **Resources** column of the **Monitor** tab displays the following values when applicable.

- ExpenseReport
- TravelRequest
- InvoiceCapture
- Receipt
- Trip
- UserProfile

Requesting a Report on Who is Viewing and Changing Personal Data

Change Logging Access

Users can ask to view a report showing change logging for their personal data (only). The log shall reflect which personal data has been changed with the following information:

- The user who is changing the data, the date and time of change, the data sets' identifying keys and their values, and the heading name for the attribute that has been changed.

To access the change logging, users should submit a Customer Support case asking that the change audit logging be queried for any changes to personal data.

View Logging Access

Users can ask to view a report showing an audit log that records who may have viewed their personal data. The log shall reflect which user, by their empid value, has viewed their personal data.

To access the view logging, users should submit a Customer Support case asking for a report detailing who has viewed a user's personal data.

